Please type a plus sign (+) inside this box → [+]

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/628,729
Filing Date	July 28, 2003
First Named Inventor	Eisentraeger
Group Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	MS1-1280US

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		EISENTRAGER, KIRSTEN et al., "Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation," Topics in Cryptology, CT-RSA 2003, Marc Joye (Ed), pp. 343-354, LNCS 2612, Springer-Verlag, 2003.	
		BONEH, DAN, et al., "Identity-Based Encryption from the Well Pairing," SIAM J. COMPUT., Vol 32, No. 3, pp. 586-615, 2003 Society for Industrial and Applied Mathematics.	
		MENEZES, ALFRED J., et al., "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," (0018-9448/93 1993 IEEE, IEEE Transactions on Information....), 8 pages.	
		FREY, GERHARD et al., "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Mathematics of Computation, Vol. 62, No. 206, April 1994, pp. 865-874.	
		HESS, FLORIAN et al., "Two Topics in Hyperelliptic Cryptography," S. Vaudenay & A. Youssef (Eds.): SAC 2001, LNCS 2259, pp. 181-189, 2001.	
		~~BONEH, DAN, et al., "Short signatures from the Weil pairing," pp. 1-17.~~ undated	
		GALBRAITH, STEVEN D. et al., "Implementing the Tate Pairing," Mathematics Dept., Royal Holloway, University of London, Egham, Surrey, UK & Hewlett-Packard Laboratories, Bristol, Filton Road, Stoke Gifford, Bristol, UK, pp. 1-14. undated	
		CANTOR, DAVID G., "Computing in the Jacobian of a Hyperelliptic Curve," Mathematics of Computation, Vol. 48, No. 177, January 1987, pp. 95-101.	
		BARRETO, PAULO S.L.M., et al., "Efficient Algorithms for Pairing-Based Cryptosystems," Universidade de Sao Paulo, Escola Politecnica, Sao Paulo (SP), Brazil & Computer Science Department, Stanford University, USA, pp. 1-16. undated	
		JOUX, ANTOINE, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems (Survey),"C. Fieker and D.R. Kohel (eds.): ANTS 2002, LNCS 2369, pp. 20-32, 2002 (Springer-Verlag Berlin Heidelberg 2002).	

Examiner Signature	/Carl Colin/	Date Considered	07/22/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C./